Móviles y Privacidad

Directrices para el diseño de privacidad en el desarrollo de aplicaciones

Índice

Junio 2012

Introducción

Antecedentes

La aparición de plataformas móviles abiertas y la convergencia de móvil y web han creado ecosistemas vibrantes y dinámicos que permiten a los individuos presentar y dar forma en la red a identidades personales muy elaboradas, conectar con aquellas comunidades de su elección y entablar contactos con aplicaciones y servicios innovadores. Una gran parte de estas posibilidades se debe al acceso en tiempo real y a la utilización de información personal que habitualmente se transfiere globalmente entre aplicaciones, dispositivos y empresas.

Estas funciones sirven como un potente catalizador para modelos de negocio innovadores y para la personalización de aplicaciones y servicios, pero también pueden servir de vehículo para un acceso malicioso o furtivo a la información personal del usuario. Incluso las aplicaciones que acceden legítimamente y usan la información personal no consiguen cumplir con *las expectativas de privacidad de los usuarios y minan su confianza en las organizaciones y en el conjunto del ecosistema móvil*. Los problemas surgen cuando a los usuarios no se les da una información clara y transparente sobre el acceso y uso de su información privada por parte de las aplicaciones o cuando no se les da la oportunidad de manifestar una elección inequívoca y un control sobre el uso de su información para fines secundarios que van más allá de las operaciones necesarias de una aplicación o servicio.

La GSMA publicó recientemente una serie de principios universales de privacidad móvil que describen de qué forma se puede respetar y proteger la privacidad de los usuarios de móviles. Estas directrices buscan articular esos principios en términos vigentes, para el diseño de aplicaciones móviles.

Alcance

Estas directrices aplican los principios de diseño de privacidad a las aplicaciones y sus servicios derivados, diseñadas para dispositivos móviles. Están pensadas para que sean aplicadas por todas las partes implicadas en la cadena de abastecimiento de aplicaciones y servicios que son responsables de la recopilación y proceso de datos personales del usuario – desarrolladores, fabricantes de dispositivos, plataformas, empresas responsables de sistemas operativos, operadoras móviles, anunciantes y empresas de estadística.

Objetivo

Las aplicaciones y sus servicios derivados deberían posibilitar experiencias positivas en el ámbito de la privacidad y generar confianza. La clave para conseguir este objetivo es un marco firme y efectivo de protección de la privacidad, basado en los principios de transparencia, capacidad de elección y control.

Estas directrices adoptan un enfoque de *Privacidad por Diseño* y están pensadas para ayudar a que se asegure que las aplicaciones móviles son desarrolladas de tal forma que se respete la privacidad de los usuarios y su información personal. La *Privacidad por Diseño* también reconoce que los usuarios tienen intereses en el campo de la privacidad (expectativas, necesidades, deseos y preocupaciones) que deben ser tratadas de forma

activa desde el principio y no como un añadido o pensamiento posterior. Las directrices animan al desarrollo, suministro y operatividad de aplicaciones móviles que pongan a los usuarios en primer lugar y les ayuden a entender (aunque sea básicamente):

- qué información personal puede acceder, recopilar y usar una aplicación móvil,
- qué información será usada para qué y por qué, y
- cómo pueden los usuarios ejercitar su libertad de elección y control sobre este uso.

Se proporcionan ejemplos de cada directriz y algunos casos prácticos ilustrativos en un anexo separado.

Definiciones

Consentimiento activo: significa que se le da al usuario una posibilidad clara de aceptar un uso específico y notificado de sus datos personales. El consentimiento activo se aplicaría cuando hay un uso secundario y no obvio de la información personal del usuario y/o en aquellas aplicaciones que tienen unas implicaciones de privacidad adicionales para los usuarios, tales como la solicitud de localización del usuario por parte de la aplicación, siempre que esa información no sea necesaria para el funcionamiento de la aplicación. El consentimiento activo debe ser mostrado de tal forma que su aceptación no sea la opción predeterminada.

Aplicación: allí donde se use el término aplicación o "App", se hace con un enfoque amplio; puede referirse a un aplicación nativa, una aplicación o script que funcionan por un periodo determinado o un widget o script que funcionan en el entorno de un navegador.

Datos de localización: información que identifica la localización geográfica del dispositivo del usuario. Puede incluir GPS, Wi-Fi, el ID del celular u otras informaciones menos granulares tales como un pueblo ciudad.

Información personal: hay infinidad de definiciones legales de información personal, pero en sus términos más sencillos hace referencia a la información referida a un individuo que puede ser utilizada para identificarle, contactarle o localizarle.

La información personal puede incluir:

- datos recopilados directamente del usuario, por medio de una interfaz de usuario de la aplicación (nombre, dirección, fecha de nacimiento)
- datos reunidos indirectamente tales como el número de teléfono, el IMEI o el UDID
- datos recopilados acerca del comportamiento, tales como datos de localización, historial de navegación o aplicaciones usadas, que están asociados a un perfil único
- datos generados por el usuario, tales como listas de contactos, vídeos y fotos, mensajes, emails, notas y registros de llamadas.

Para ser identificado, un individuo no tiene por qué ser conocido por su nombre –un usuario puede ser identificado incluso cuando su información se asocia sólo con un único identificador, como por ejemplo el Identificador Único de Dispositivo.

Hay categorías de información que pueden ser consideradas "**sensibles**" y que pueden necesitar de una seguridad adicional. Estas pueden incluir, por ejemplo, datos de acceso y registro, información financiera o aquella referida a la salud de la persona.

Privacidad: es un concepto dinámico que puede significar cosas diferentes para distintas personas. Teniendo en cuenta los propósitos de estas directrices, la privacidad se define como la capacidad que tienen los individuos de conocer como se recopilará, compartirá y usará su información personal y su capacidad de elección y control sobre su uso.

Usuario: el usuario final de aplicaciones y servicios derivados.

Transparencia, capacidad de elección y control — situando al usuario en primer lugar

Un aspecto clave a la hora de fomentar la confianza en las aplicaciones es ser abierto con los usuarios y permitirles conocer:

- quién está recopilando y utilizando su información personal
- por qué se utiliza información personal
- qué información personal está siendo compartida, con quién y con qué propósitos.

Los usuarios deberían tener la información suficiente para tomar una decisión informada sobre el uso de una aplicación y las consecuencias de hacerlo. Parte de esta información puede ser obvia antes de que el usuario descargue o active una aplicación, por lo que las explicaciones adicionales sobre la aplicación no son necesarias.

Resumiendo:

- **Sea transparente:** diga a los usuarios quién es, qué información personal necesita, qué tiene pensado hacer con ella y con quién piensa compartirla (y por qué) — ¡pero no los sature con mensajes instantáneos!
- **Ayude a los usuarios a controlar su privacidad:** hágales saber cuáles son los ajustes predeterminados de la aplicación
- **Haga fáciles de entender a los usuarios las opciones y mecanismos para controlar la privacidad:** hágaselo fácil y no difícil— si lo hace, su propuesta les gustará aún más

Directriz	Ejecución	Casos prácticos y ejemplos
TEC1 **No acceda a/o recopile información personal de forma clandestina.** Una aplicación no puede acceder ni recopilar información personal de sus usuarios de forma secreta. Los usuarios deben ser informados de la recopilación y uso de su información personal desde el inicio, permitiéndoles tomar decisiones informadas sobre el uso de una aplicación o servicio.	Antes de que un usuario descargue o active una aplicación, debe ser informado de: • qué información personal va a acceder, recopilar y usar una aplicación • qué información personal será almacenada (en su dispositivo y de forma remota) • qué información personal será compartida, con quién será compartida y con qué propósito • por cuánto tiempo se almacenará esa información personal • cualquiera de los términos y condiciones de uso que afecten a la privacidad del usuario. Avise al usuario y haga esta información fácil de encontrar y entender. Hágala sencilla y facilítele la capacidad de elección. Permita que el usuario rechace la instalación o activación si no desea que su información personal sea usada en los términos que le han sido explicados. Garantice la usabilidad y evite un exceso de mensajes instantáneos que agobien al usuario. Tenga en cuenta cuál va a ser la experiencia del usuario.	Una aplicación no puede acceder a la localización del usuario si esa aplicación no es una aplicación de servicios basados en localización. Si la información de localización es secundaria para la aplicación y se necesita para cumplir con otros fines comerciales, se tiene que contar con el consentimiento activo del usuario (ver la sección "Privacidad de la localización" más abajo). Una aplicación no puede acceder y usar los datos de los contactos guardados en la agenda de ningún dispositivo móvil, a no ser que sea una parte funcional de la aplicación y haya sido explicada claramente al usuario. La transparencia es la clave. Dígale a los usuarios qué información necesita y por qué — y mantenga su palabra. Si cambia de opinión posteriormente y desea utilizar la información personal para otros propósitos distintos de los que manifestó a sus usuarios en un principio, tendrá que volver a ponerse en contacto con ellos, informarles acerca de los nuevos usos y conseguir su permiso.

Directriz	Ejecución	Casos prácticos y ejemplos
TEC2 **Identifíquese a los usuarios** Los usuarios tienen que saber quién está recogiendo o usando su información personal y cómo pueden ponerse en contacto con esa entidad para conseguir más información o para ejercer sus derechos.	Antes que un usuario descargue o active una aplicación, debe ser informado de la identidad de cualquiera de las entidades que recogerán o usarán su información personal dentro del ámbito de la aplicación, incluyéndose el nombre de la empresa o persona y el país de origen. Los usuarios deben contar con acceso fácil (por medio de un link o uno de los apartados del menú) a los datos de contacto de la organización.	La página de inicio de la aplicaciones es un lugar excelente para publicar los puntos clave en materia de privacidad, información de contacto y para proporcionar un enlace a un informe más detallado sobre privacidad. No hay una solución única para proporcionar a los usuarios información sobre usted, su empresa, la privacidad del usuario y qué va a hacer con sus datos personales. Sea creativo y anime a los usuarios a que exploren las mejores maneras de controlar su privacidad — pero no les agobie y hágaselo sencillo y fácil.
TEC3 **Deje que los usuarios ejerzan sus derechos** Proporcione a los usuarios información suficiente, de forma que sea razonable pensar que saben cómo acceder y corregir cualquier información personal que pueda almacenar sobre ellos.	Proporcione un informe breve y realmente informativo, explicando en términos claros y sencillos cómo puede conseguir el usuario una copia de su información personal o corregir y actualizar la información proporcionada por ellos mismos o que usted almacena.	Como se indica previamente, la página de inicio de la aplicación puede ser el lugar idóneo para ubicar un aviso claro y sencillo para los usuarios o para dirigirles a un apartado con información más detallada sobre como ejercer su derecho a la protección de datos.
TEC4 **Minimice la información que recopila y limite su uso.** La información recopilada por una aplicación debe ser razonable, no excesiva, y usada dentro del ámbito de las expectativas del usuario y otros propósitos legítimos de la empresa, tal y	Piense qué información necesita y luego justifíquelo. ¿Es realmente necesaria?, ¿tiene que recopilarla, compartirla o almacenarla para cumplir con una necesidad de empresa u obligación legal? Una aplicación tiene que acceder, recopilar y usar únicamente la mínima información requerida para: • generar, operar o mantener la aplicación • cumplir con los objetivos identificados de la	Si necesita acceso a los datos de una lista de contacto, identifique que campos se necesitan obligatoriamente para que se desempeñe una función específica de la aplicación y no recopile más que los campos requeridos. No use esa información para otros propósitos que no sean obvios, a no ser que el usuario haya accedido a esta utilización.

Directriz	Ejecución	Casos prácticos y ejemplos
como se notificó a los usuarios.	empresa, sobre los que ha informado a los usuarios o para cumplir con las obligaciones legales. Use la información personal de la manera que los usuarios esperarían, si tomasen la decisión de descargar o activar una aplicación.	
TEC5 **Cuando fuese necesario, obtenga el consentimiento activo del usuario** En algunas ocasiones los usuarios tienen que dar su consentimiento activo para el uso de su información personal. Recopilación o uso de información personal que no es necesaria para el propósito principal de la aplicación	En la mayoría de los casos, será obvio para los usuarios qué información personal será necesaria como soporte de la aplicación. Sin embargo, allí donde el acceso, recopilación y uso de la información personal no sea necesario para el propósito principal de la aplicación y pudiera ser inesperado por los usuarios, éstos deben tener la oportunidad de decidir si quieren permitir esos usos secundarios y no obvios de su información. Hay otras situaciones que pueden requerir también de un consentimiento activo: redes sociales y medios digitales, publicidad móvil, servicios de localización, niños y adolescentes (tal y como se detalla en otras secciones debajo). Allí donde sea necesario contar con el consentimiento activo, los usuarios deberían ser informados de: • por cuánto tiempo es válido ese consentimiento • cómo pueden administrar ese consentimiento que han dado • las consecuencias de mantener o retirar su	Las aplicaciones que no usan los servicios de localización para ninguna de sus funciones u operatividad contratadas por el usuario, no deberían recopilar esta información para otros propósitos -por ejemplo, publicidad dirigida o estadísticas- a no ser que el usuario brinde su consentimiento activo.

Directriz	Ejecución	Casos prácticos y ejemplos
	• consentimiento. Los usuarios tienen que poder retirar su consentimiento de una forma simple y eficiente, sin esperas o costes indebidos.	
a) Compartir información personal con terceros	Si terceras partes recopilarán o tendrán acceso a la información del usuario para sus propios propósitos, el usuario tiene que ser informado lo antes posible de que sus datos serán compartidos, indicando: • con quién serán compartidos y con qué fines • enlaces para ponerse en contacto con esas terceras partes y sus informes de privacidad. Los usuarios deben tener la opción de elegir si quieren permitir esa recopilación, acceso y uso por terceros.	Las aplicaciones no deberán incluir un código de terceros que recopile y analice información personal para dirigir publicidad a los usuarios, sin el consentimiento activo del usuario.
b) Almacenar información personal inmediatamente después del uso de la aplicación.	Si los datos de un usuario se retienen inmediatamente después del uso de una aplicación, los usuarios tiene que ser informados sobre: • los periodos durante los que se almacenará la información y por qué • cómo puede ejercitar el usuario sus derechos específicos sobre su información.	
TEC6 **Dé control a los usuarios sobre la frecuencia de los mensajes instantáneos.**	Siempre que sea posible, dé a los usuarios la posibilidad de decidir cómo y con qué frecuencia recibirán mensajes instantáneos para la toma de decisiones referentes al acceso y uso de su	Los usuarios deben tener la opción de "recordar" sus datos de acceso, dirección de facturación, direcciones de correo electrónico o su localización. Es posible proporcionar una cobertura de aviso automático única para cada tipo de dato

Directriz	Ejecución	Casos prácticos y ejemplos
Siempre que sea posible, los usuarios deberían tener la opción de decidir cómo -y con qué frecuencia- se les recuerda qué funciones y procesos usan su información personal.	información personal. Privacidad por Diseño significa poner al usuario en primer término y ayudar a que sea consciente de las implicaciones de privacidad que tienen las aplicaciones y servicios y que las administre, de forma que se mejore la experiencia de privacidad del usuario.	o granular avisos automáticos de contexto más específico. Por ejemplo, los usuarios pueden tener la opción de permitir que una aplicación acceda de forma permanente a los servicios de localización del dispositivo o durante un periodo específico o seleccionar que se les avise periódicamente de esta circunstancia por medio de un email, un mensaje de texto, una notificación de la aplicación o un icono.
TEC7 **No a las actualizaciones silenciosas ("secretas")** Los usuarios deben aceptar cualquier cambio en una aplicación que afecte a su privacidad.	Los usuarios tienen que ser informados sobre cualquier cambio substancial en la forma que una aplicación recopila o usa su información personal, antes de que el cambio sea llevado a cabo, de forma que puedan tomar una decisión informada sobre si desean continuar utilizando la aplicación. El consentimiento para esos cambios puede ser obtenido de dos formas: 1. Para aquellos cambios que son esenciales para que la aplicación continúe funcionando: notifique que se llevará a cabo un cambio y de la posibilidad de desactivar la aplicación. 2. Para aquellos cambios en los que el usuario pueda elegir si los adopta: un mensaje instantáneo con las opciones de si desea permitir los cambios o continuar con la configuración previa.	Esto no impide las actualizaciones remotas de tipo inalámbrico que son necesarias para mantener la operatividad principal e integridad de una aplicación o servicio. La directriz **se aplicaría**, por ejemplo, siempre que la aplicación deseara de repente acceder y subir los datos de contacto almacenados en el dispositivo móvil o los datos de localización del dispositivo.

Almacenamiento de datos y seguridad

Puede haber seguridad sin privacidad, pero no puede haber privacidad sin seguridad. Asegúrese de que está protegiendo adecuadamente la información personal que un usuario le ha confiado; en el teléfono móvil y allí donde usted guarde o desde donde transmita información personal.

Piense por qué necesita retener la información personal de un usuario y por cuánto tiempo necesita tenerla almacenada, ¿puede justificarlo? La información personal almacenada indefinidamente pierde valor con el paso del tiempo, pero incrementa su coste y su riesgo. Identifique por cuánto tiempo es necesaria (por contraposición a deseable) una información personal determinada para su modelo de negocio y asegúrese de eliminarla de forma segura cuando ya no sea requerida. Establecer periodos de almacenamiento para sus datos (tan breves como sea posible) es una buena decisión de negocio, puede ayudarle a controlar riesgos y costes y a evitar acciones de los reguladores o publicidad negativa si algo saliera mal (porque la almacenó por demasiado tiempo y los datos fueron puestos en peligro).

Directriz	Ejecución	Casos prácticos y ejemplos
ADS1 **Administración activa de los identificadores.** Siempre que una aplicación cree o use un identificador único, tome medidas para asegurarse de que el identificador está asociado al usuario legítimo de la aplicación y mantenga esta información actualizada.	Cada una de las partes que usa identificadores es responsable de tomar medidas para: • asegurarse de que un identificador único se asocia con un usuario único • asegurarse de que los identificadores únicos se almacenan actualizados y sólo por el tiempo necesario para cumplir con los propósitos y razones notificadas a los usuarios • evitar que un identificador único se asocie con otro usuario a no ser que sea necesario por una necesidad de negocio justificada (Ver *Casos prácticos y ejemplos)*	Las operadoras móviles pueden reasignar identificadores tales como MSISDN (números móviles) a otros clientes sin que la aplicación lo sepa. Si usted capta el MSISDN de un usuario debe tomar medidas para asegurarse de que esa información es correcta y está actualizada mediante confirmaciones periódicas con el usuario. Asimismo, los fabricantes de dispositivos deben asignar un Identificador Único de Dispositivo (UDID). Los usuarios de móvil pueden reemplazar su teléfono móvil y venderlo a otros individuos. A no ser que se tenga cuidado, el nuevo propietario del móvil podría estar fácilmente asociado con el Identificador Único de Dispositivo u otros identificadores únicos asociados con el dueño anterior. Esta asociación y vínculo podría tener consecuencias en las experiencias de privacidad en la red del nuevo usuario y en su utilización del dispositivo. Cada una de las partes

Directriz	Ejecución	Casos prácticos y ejemplos
		que recopila y usa UDIDs es responsable de asegurar que se cumple con esta directriz.
ADS 2 **Mantenga la información protegida.** Tome las medidas apropiadas para proteger la información personal del usuario de accesos o revelaciones no deseados.	Tome medidas técnicas y decisiones de negocio que eviten la mala utilización o alteración de la información personal. Siempre que una aplicación cree o recopile información personal considerada **confidencial,** como datos de acceso, UDIDs, números de móvil, datos de contacto, información financiera… esa información debe ser guardada y transmitida de forma segura.	Recopilar y guardar cierta información cuando es sencillamente innecesario crea el riesgo de que se pierda, sea robada y mal utilizada. Si necesita recopilar, transmitir y retener información confidencial como pueden ser los datos de pago de un usuario o sus datos de acceso, deberá hacer esta información segura mediante encriptación o un mecanismo adecuado de función hash y borrar esa información cuando ya no sea necesaria.
ADS 3 **Autentique allí donde las medidas de seguridad lo exijan.** Autentique a los usuarios siempre que sea posible usando métodos de autenticación ajustados a los riesgos.	Siempre que la reafirmación de la identidad del mundo real sea un componente importante de un servicio, se deberá desarrollar una autenticación más sofisticada, como la autenticación de dos factores usando un teléfono móvil y UICC. Considere la utilización de CAPTCHAs y RE-CAPTCHAs para poder diferenciar miembros genuinos de aquellos que sólo generan spam. Use las herramientas técnicas para restringir el spidering (o araña web) y las descargas colectivas o el acceso sin el permiso de la red.	
ADS4 **Fije periodos de almacenamiento y eliminación.** La información personal que se va a guardar debe estar sujeta a periodos de almacenamiento y eliminación,	Justifique la recopilación y almacenamiento de información personal de acuerdo con necesidades de negocio claramente identificadas u obligaciones legales. Fije una política de actuación y aplíquela a nivel técnico y de procesos de negocio.	Los datos almacenados en un perfil de conducta relacionados con un usuario único por medio de cookies u otro identificador de dispositivo, incluso si no existe otra información identificable, no deben ser considerados realmente anónimos. Un perfil con el identificador único eliminado o hacheado puede considerarse anónimo.

Directriz	Ejecución	Casos prácticos y ejemplos
justificados por necesidades de negocio claramente identificadas u obligaciones legales.	Una vez que la información personal ya no es necesaria para cumplir con un objetivo de negocio específico y legítimo o con requerimientos/obligaciones legales, debe ser destruida o pasar a ser anónima. Los datos verdaderamente anónimos pueden ser almacenados indefinidamente. Para convertir una serie de datos en anónimos, elimine cualquier información que pueda servir para identificar a un individuo en concreto, asegurándose de que no es posible identificar a ese individuo de nuevo y asegurándose de que esos datos no pueden relacionarse, por medio de identificadores únicos, con un individuo específico no identificado.	

Educación

Es importante que los usuarios entiendan cómo administrar su privacidad y proteger su información personal de la mejor manera posible, mediante una información clara y sencilla sobre las opciones de privacidad y seguridad de las aplicaciones. Se trata de ayudar a los usuarios a que sean conscientes de los distintos aspectos de la privacidad y la seguridad y cómo administrarlos.

Directriz	Ejecución	Casos prácticos y ejemplos
E1 **Forme a los usuarios en las implicaciones y opciones de privacidad de su aplicación o servicio y en cómo pueden administrar su privacidad.**	Proporcione información a los usuarios sobre las opciones de privacidad y seguridad y las funciones de las aplicaciones y servicios y cómo activarlas y administrarlas para ayudar a los usuarios a proteger y controlar su propia privacidad. Esta información debería estar claramente indicada, usando un lenguaje sencillo y claro. A los usuarios se les debe dar detalles de cómo proteger su privacidad en general, principalmente por medio de enlaces a fuentes y páginas web en la red.	Los usuarios pueden ser dirigidos a las páginas de seguridad de una tienda o desarrollador de aplicaciones o a otras iniciativas que dan claves sobre teléfonos inteligentes y seguridad y privacidad de las aplicaciones, como: http://alertaenlinea.gov/articulos/s0018-aplicaciones-m%C3%B3viles-qu%C3%A9-son-y-c%C3%B3mo-funcionan - www.staysafeonline.org/in-the-home/mobile-devices www.getsafeonline.org

Redes sociales y medios sociales

Las aplicaciones de interacción social permiten a los usuarios conectarse y compartir información con una comunidad formada por otros usuarios o con el público general. Este tipo de aplicaciones pueden conllevar implicaciones de privacidad importantes y deberían incluir opciones de protección de la privacidad de forma predeterminada e instrucciones e información clara para los usuarios sobre cómo afectan a su privacidad las decisiones que toman.
Es importante asegurarse de que los usuarios puedan tomar decisiones plenamente informadas sobre la utilización de servicios de redes sociales y que puedan tener las opciones de privacidad apropiadas.

Directriz	Ejecución	Casos prácticos y ejemplos
RSMS1 **Invite a los usuarios a que se registren en redes sociales, pero tenga cuidado con el mapeo en perfiles públicos de la información de registro.**	Ponga como requisito a los usuarios la creación y registro de una cuenta antes de usar el servicio e indique claramente al usuario qué información es voluntaria. No mapee automáticamente la información de registro del usuario al perfil público del mismo, a no ser que el usuario haya sido informado de ello y se le haya dado la opción de decidir y el control. Ver debajo.	Si la opción predeterminada de privacidad de una red social es "pública", los usuarios deberían ser informados antes de que faciliten cualquier tipo de información personal y creen una cuenta y tienen que tener la opción de aceptarla o rechazarla.
RSMS2 **Asegúrese de que las opciones predeterminadas protegen la privacidad y dan control a los usuarios sobre sus perfiles personales de una forma fácil de entender y usar.**	Los usuarios deben ser informados de forma clara y transparente sobre la configuración de privacidad de su perfil y sobre la forma en que sus datos serán compartidos o estarán disponibles para otros. Los usuarios deben saber: • qué información o categorías de información suyas serán publicadas al finalizar el registro • cómo pueden cambiar fácilmente la configuración predeterminada • si su información personal y ellos mismos podrán ser • encontrados por otros usuarios o estos serán alertados • cómo pueden hacer para que sus datos "privados" sean visibles sólo por las partes autorizadas.	Es una buena idea facilitar una página educativa de privacidad para ayudar a los usuarios a entender cómo pueden administrar su privacidad. Se puede incluir un apartado que indique que la información que hagan pública será rastreable por medio de motores de búsqueda.

Directriz	Ejecución	Casos prácticos y ejemplos
	Tiene que quedar claro de forma intuitiva para los usuarios qué información de sus perfiles es pública, qué información se publica para un grupo limitado (como por ejemplo los amigos) y qué información es completamente privada (sólo visible por el usuario). Los usuarios tienen que tener la posibilidad de revisar toda la información de sus perfiles, incluyendo los datos generados por el usuario, los de uso y los derivados.	
RSMS3 **Tome medidas para evitar que los niños se pongan en peligro a sí mismos.** Los usuarios menores de edad requieren más medidas de privacidad predeterminadas y otras medidas de protección adicionales.	Las leyes nacionales o códigos reguladores que se apliquen pueden requerir que los usuarios menores de una cierta edad tengan unas opciones predeterminadas de "protección de la privacidad" más privadas y que se les dé información de una forma muy clara y sencilla. Tiene que impedirse que los niños publiquen datos de contacto o su localización exacta.	Esta directriz no tiene que ver con la verificación de la edad de los niños, sino con ayudarles a entender las implicaciones de privacidad que tiene relacionarse a través de la red y cómo pueden proteger su privacidad. También hace referencia a que se asegure que los perfiles de los usuarios menores de 18 años sean privados de forma predeterminada. Los usuarios menores de 16 no deberían tener la posibilidad de publicar (esto es, compartir con el público en general) su localización exacta o sus datos de contacto.
RSMS4 **Cree herramientas adecuadas para desactivar y eliminar los datos de las aplicaciones y cuentas.**	El usuario debería tener la posibilidad de desactivar sus cuentas y tiene que ser capaz de eliminar sus cuentas, obteniendo como resultado la completa eliminación de toda su información personal y de todocontenido publicado (de la red social y cualquier otro servidor final o de backend).	Proteja de las acciones maliciosas y tome medidas para autenticar a los usuarios antes de desactivar o eliminar cuentas e información personal.

Publicidad móvil

Los usuarios ven sus dispositivos móviles como algo intrínsecamente personal y pueden tener experiencias de privacidad, expectativas e intereses diferentes a los de los consumidores online "fijos" (de línea fija).

Mientras la publicidad está siendo objeto de una regulación y los estándares auto regulatorios sobre el uso de la información personal para propósitos publicitarios van en aumento, varios estudios han mostrado que dar a los usuarios información detallada sobre cómo se elige la publicidad que ven y darles un mayor control sobre cómo se les segmenta y categoriza, les lleva a estar más cómodos y a aceptar mejor los anuncios personalizados.

La clave para hacer crecer la publicidad en el móvil y asegurarse de que los anuncios son relevantes y útiles para los usuarios es desarrollar las mejores prácticas, basadas en una transparencia real y en control y capacidad de elección significativa.

Directriz	Ejecución	Casos prácticos y ejemplos
PM1 **Informe a los usuarios de las opciones publicitarias.** Deje que los usuarios sepan si una aplicación está financiada por anuncios antes de que la descarguen y/o la activen.	Informe a los usuarios de si existe la posibilidad de que se ponga publicidad en o alrededor de una aplicación. Se aplica tanto si la aplicación es gratuita para el usuario como si es de pago.	Muchas aplicaciones son gratuitas y se financian mediante publicidad. Lo usuarios pueden no ser conscientes de este hecho antes de que se descarguen o activen las aplicaciones. Puede informarles por medio de un "icono de anuncio" y/o un breve "aviso". El icono o aviso puede enlazarse con una URL que informe de forma más detallada para ayudar a los usuarios a entender qué información será usada y qué opciones tienen en materia de publicidad. Esto podría ayudar a reforzar la opinión que tienen de usted y a que se genere confianza, en usted y sus aplicaciones y en sus socios o "tiendas de aplicaciones".
PM2 **Cree un acuerdo apropiado de publicidad personalizada para el usuario.** Los usuarios tienen que aceptar la publicidad personalizada y dar un	Antes de que recopile cualquier información personal, deje que los usuarios sepan que habrá publicidad personalizada para ellos, cuándo y dónde aparecerá esa publicidad y qué información será usada.	Un usuario no tiene que aceptar cada vez, puede dar su consentimiento una sola vez. Lo que es importante es que el usuario tenga la información suficiente y todas las opciones para tomar una decisión informada.

Directriz	Ejecución	Casos prácticos y ejemplos
consentimiento activo para ser categorizados entre aplicaciones o por terceras partes.	Si una aplicación va a desarrollar un perfil único de los intereses del usuario, basado en el comportamiento del usuario con la aplicación y este perfil va ser usado para publicidad personalizada, los usuarios tienen que ser informados de que se va a llevar a cabo esa personalización y creación de perfil y deben aceptarlas. Se tienen que dar instrucciones claras a los usuarios acerca de cómo modificar o eliminar un perfil y cómo quedar **excluidos** de esa personalización y categorización. Si el perfil del usuario se construye con la actividad que se desarrolla fuera del ámbito de una aplicación y no fuera razonable que los usuarios esperasen esa conexión con el uso de otras aplicaciones, el usuario tiene que ser informado del espectro de datos que se recopila y usa para esa categorización o perfil y tiene que dar su consentimiento activo. Si la categorización y personalización es llevada a cabo por terceros (por ejemplo, una red o una compañía a de estadística móvil), los usuarios tienen que dar su consentimiento activo de forma que autoricen a terceras partes a recopilar y usar su información.	Un usuario descarga y utiliza una aplicación llamada “coffee2go”. La aplicación recopila ciertos datos del dispositivo y cierta información sobre el comportamiento del usuario con la aplicación y crea un perfil de esos usos, con la intención de hacer llegar publicidad basada solamente en la información contenida en este perfil. El usuario tiene que haber aceptado de forma activa estos términos después de haber sido informado sobre la categorización y la publicidad personalizada. PERO, la entidad responsable de la aplicación "coffee2go” y de recopilar y categorizar la información del usuario relacionada con esta aplicación, **también** tiene pensado construir un "perfil combinado de usuario" que se basa en los datos reunidos a partir del comportamiento del usuario con otras aplicaciones, tales como "pizza2go". Se quiere hacer llegar al usuario publicidad basada en este perfil de usuario "combinado". El usuario **tiene** que ser informado de esta situación desde el principio y debe dar su consentimiento activo antes de que cualquier actividad de categorización o publicidad personalizada comience.
PM3 **Personalización basada en la recopilación legítima de datos.** La publicidad puede personalizarse basándose sólo en la información personal que es necesaria para la	La publicidad personalizada para el usuario basada en información recopilada del teléfono móvil (por ejemplo, la localización) o en la interacción del usuario con otras aplicaciones o internet sólo puede utilizar la información que ha sido recopilada mientras se proporcionaban las funciones y operatividad que el usuario demandó.	Esto permite tener en cuenta aplicaciones diseñadas específicamente para hacer llegar ofertas publicitarias a los usuarios, basadas en sus preferencias e intereses.

Directriz	Ejecución	Casos prácticos y ejemplos
función principal de la aplicación.		
PM4 **Respete la privacidad en casos de marketing viral.** El marketing viral debe darse sólo tras el consentimiento activo del usuario.	Respete la privacidad de la red de contactos del usuario. Las aplicaciones no deben recopilar información sobre los contactos del usuario o enviarles mensajes sin el consentimiento activo del usuario, para participar en cualquier actividad de uso compartido o de marketing que una aplicación pueda incluir.	
PM5 **Asegúrese de que el contenido es apropiado.** La publicidad no personalizada debe ser apropiada para un público general. El contenido de la publicidad debe ser apropiado para los rangos de edad potenciales o la edad conocida del usuario.	Si una aplicación está clasificada como autorizada para usuarios jóvenes, cualquier publicidad que se facilite en la aplicación o alrededor de la misma tiene que ser apropiada para la edad mínima autorizada y el público objetivo y acatar las leyes, códigos o regulaciones aplicables. Ver la sección sobre niños más abajo	Por ejemplo, si una aplicación está autorizada para niños a partir de 7 años, cualquier publicidad que se inserte en la aplicación o alrededor de la misma tiene que ser válida para la mínima edad permitida (en el ejemplo, 7 años). En este ejemplo se debería contar además con el consentimiento de los padres o tutores legales.

Localización

La utilización de datos de localización sigue generando importantes preocupaciones sobre la privacidad del usuario. La privacidad de la localización es especialmente importante para los usuarios de móviles. Es importante asegurar que los usuarios tienen oportunidades para manifestar una elección real sobre si su localización puede ser accedida y compartida por las aplicaciones.
Ver también: *Publicidad móvil*.

Directriz	Ejecución	Casos prácticos y ejemplos
L1 **Informe al usuario de que la localización será usada y de l posibilidades.** Las aplicaciones sólo pueden acceder, usar y compartir los datos de localización tras un acuerdo previo e informado.	Antes de que se acceda y utilice la localización del usuario, las aplicaciones basadas en la localización tienen que mostrar un aviso claro con: • a qué datos de localización va a tener acceso la aplicación (ID del teléfono, GPS, ciudad o pueblo) • cómo serán usados esos datos • si los datos serán almacenados y por cuánto tiempo • con quién serán compartidos esos datos. Si la aplicación llevase a cabo una comprobación única de localización activa del usuario, para proporcionar un servicio solicitado por el usuario y este es el único propósito de la aplicación, entonces **no es necesario proporcionar ninguna información suplementaria relacionada con la privacidad o contar con un consentimiento específico del usuario.**	Si un usuario descarga o activa una aplicación llamada "Donde está mi cajero más cercano", para que ese servicio pueda localizar el dispositivo del usuario y decirle donde se encuentra el cajero automático más cercano, no hay necesidad de darle al usuario ninguna información adicional sobre privacidad o conseguir su consentimiento activo (ya que el consentimiento está claro y está implícito en la solicitud del usuario). Sin embargo, si la aplicación almacena la localización y cualquier otra información contextual sobre las solicitudes del usuario para construir un perfil y crear publicidad personalizada para el usuario más adelante, entonces la aplicación debería informar al usuario de estos términos y conseguir su consentimiento activo antes de que la información del usuario sea recopilada y usada para esos propósitos. Ver más abajo.

Directriz	Ejecución	Casos prácticos y ejemplos
L2 **Obtenga las autorizaciones adecuadas para el uso de datos de localización.** Algunos usos de los datos de localización requieren que se les dé a los usuarios información adicional sobre privacidad y obtener su consentimiento activo.	Si una aplicación va a almacenar un **historial** con las localizaciones del usuario, el usuario debe ser informado y también sobre por cuánto tiempo se almacenarán esos datos y por qué. Los usuarios deben dar su consentimiento activo para que se almacene un historial asociado a ellos como individuos únicos y tienen que tener la posibilidad de revisar y borrar ese historial.	
	Si los usuarios van a recibir **publicidad** o resultados patrocinados basados en su localización contextual, tiene que mostrárseles un aviso claro que indique que la aplicación se financia con publicidad. Si los usuarios van a recibir publicidad o resultados patrocinados basados en un historial almacenado de localizaciones del usuario, el usuario tiene que dar su consentimiento activo.	
	Si una aplicación continúa recopilando, usando o compartiendo datos de localización durante el funcionamiento de la aplicación o después de que el usuario ha cerrado la aplicación: los usuarios tienen que dar su consentimiento activo para el funcionamiento continuado de la función de localización • la aplicación tiene que incluir un sistema que alerte al usuario de que la función de localización continúa operativa • una vez que la aplicación se ha cerrado no puede recopilar información de localización a no ser que el usuario haya accedido a ello. La aplicación tiene que proporcionar opciones de ajuste fácilmente accesibles que permitan al usuario activar o desactivar de forma inmediata los sistemas de localización, incluyendo una opción de "Localización desactivada" que anule todas las otras opciones de localización con que cuenta la aplicación. Si una aplicación va a publicar automáticamente la localización de un usuario o compartir la localización de un usuario con otras personas, por ejemplo	Se podría usar un símbolo para indicar que una aplicación está accediendo activamente a los datos de localización del usuario para mejorar la conciencia del usuario al respecto y darle la oportunidad de que administre su privacidad activamente. De forma alternativa, se podría enviar a los usuarios mensajes de texto periódicos o alertarles por otros medios de que su localización está siendo cuantificada.

Directriz	Ejecución	Casos prácticos y ejemplos
	mediante una función de **localización social:** • La opción predeterminada tiene que ser privada. Eso quiere decir que el usuario tiene que dar consentimiento activo para empezar a compartir la localización y tiene que elegir positivamente a los usuarios individuales o grupos de usuarios que tendrán acceso a su localización • Cuando el modo "compartir" este activado, tiene que haber un indicador claro y destacado de que la localización está siendo compartida • El usuario debe ser capaz de establecer el nivel de granularidad de su localización (por ejemplo: ciudad, calle, localización física exacta) • El usuario tiene que ser capaz de anular en cualquier momento y manualmente la información de localización que se muestra así como de apagar la opción de compartir localización • Tiene que evitarse la publicación (esto es, compartir con el público general) de la localización de los usuarios identificados como niños o cuya edad ha sido verificada. Si estos usuarios son capaces de compartir información con sus contactos, la granularidad debe estar pre-establecida a nivel de ciudad o más amplia. Si la aplicación comparte los datos de localización con otras aplicaciones, páginas o servicios: • Tiene que haber un indicador identificando y proporcionando un enlace u otros sistemas para acceder a la aplicación, pagina web o servicio • Los usuarios tienen que dar un consentimiento activo para compartir la localización con la aplicación, pagina web o servicio. El usuario tiene que ser capaz de administrar fácilmente aquello a lo que otras aplicaciones, páginas web y servicios tienen acceso, por ejemplo para retirar el permiso siempre que lo desee.	

Niños y adolescentes

Aunque los niños y adolescentes pueden tener las habilidades necesarias para navegar por internet e interactuar con aplicaciones móviles, pueden carecer de la madurez para apreciar las amplias consecuencias sociales y personales que puede tener revelar información personal o permitir a otros que la recopilen y usen.

Las aplicaciones específicamente dirigidas o usadas por niños y adolescentes tienen que asegurarse de que la recopilación, acceso y uso de la información personal es apropiada en cualquier circunstancia y es compatible con la legislación nacional y cualquier código regulatorio aplicable.
Ver también: *Redes sociales y medios digitales, Localización, Publicidad móvil*

Directriz	Ejecución	Casos prácticos y ejemplos
NA1 **Ajuste la aplicación para los rangos de edad apropiados.** Las aplicaciones destinadas a niños y adolescentes deberían ser apropiadas para los rangos de edad objetivos y ayudar a esos usuarios a entender fácilmente las consecuencias de instalar o usar una aplicación o servicio.	Considere el riego que representa para un niño o un adolescente la recopilación y utilización de información personal y asegúrese que estos riesgos son explicados apropiadamente. Asegúrese de que el lenguaje y el estilo de la aplicación son apropiados y que ayuden a que se entienda antes de que se instale y active la aplicación. Las aplicaciones tienen que mostrar un aviso claro con el contenido que estará disponible y su idoneidad para los distintos grupos de edad.	
NA2 **Instale por defecto ajustes de protección de la privacidad.** Las aplicaciones que están dirigidas a niños y adolescentes tienen que tener por defecto un ajuste de la localización que impida a los usuarios publicar de forma automática sus datos de localización exactos.	Establezca un mínimo de ajustes predeterminados para las categorías de información personal y de localización que puedan representar un riesgo para los niños y adolescentes en relación con la naturaleza de la aplicación. Limite la granularidad de la información de localización que el niño o adolescente puede compartir a un nivel genérico como ciudad o región.	Por ejemplo, no permita que se recopilen o compartan datos de contacto y localización de forma automática y limítelos para reducir riesgos asociados.

Directriz	Ejecución	Casos prácticos y ejemplos
NA3 **Acate las leyes de protección de la infancia.** Las aplicaciones deben acatar en todo momento los requerimientos legales que las jurisdicciones pertinentes puedan establecer para proteger a los niños.	En muchas jurisdicciones se aplican leyes, códigos y regulaciones específicas a la recopilación de información personal de niños y adolescentes. En algunos casos, se requiere el permiso paterno antes de que se recopile información personal de los niños. Si su aplicación está dirigida a los niños, tiene que tomar las medidas necesarias para cumplir con las normas aplicables a la recopilación y usos de su información personal.	
NA4 **Verifique la edad siempre que sea posible y apropiado.** En ciertas circunstancias la verificación de la edad puede ser apropiada (por ejemplo, cuando las aplicaciones tienen funciones de red social o permiten el acceso a contenidos para adultos).	Siempre que sea posible, integre un proceso de verificación de edad en la aplicación para poder controlar el acceso a aplicaciones o contenidos con restricciones de edad y minimizar la posibilidad de que se recoja y comparta información personal inapropiada de niños y adolescentes. Si el establecimiento de controles de acceso no es posible, entonces se tiene que pedir a los usuarios que se certifiquen ellos mismos –en este caso se les tiene que pedir su fecha de nacimiento durante la instalación, activación o registro. Tenga en cuenta que los niños y adolescentes son expertos en eludir los controles de seguridad. Si los usuarios introducen una fecha de nacimiento que les deniegue o restrinja el acceso a un servicio, debe evitarse que puedan comenzar el proceso de nuevo e introduzcan una fecha de nacimiento distinta, durante esa sesión y después de la misma, si es técnicamente posible. Asegúrese de que no incluye mensajes instantáneos para el usuario que puedan interpretarse como que los anima a mentir sobre su fecha de nacimiento.	Un campo de fecha de nacimiento con un letrero grande informando de que el acceso será restringido a los usuarios menores de 16 años, animará a los usuarios más jóvenes a mentir sobre su edad en la auto certificación.

Responsabilidad y ejecución

Para que estas directrices tengan impacto, tienen que aplicarse a todas las partes que participan del ecosistema de las aplicaciones móviles y ser desarrolladas por diseño dentro de la plataforma de la aplicación. Todo aquel que esté involucrado en el desarrollo, distribución, venta y suministro de aplicaciones, quienes acceden, recopilan o usan información personal o quienes hacen posible que otros accedan, recopilen y usen información personal, tienen que trabajar para crear herramientas e interfaces que hagan que estas líneas de actuación sean posibles.

Directriz	Ejecución	Casos prácticos y ejemplos
RE1 **Asigne responsabilidades de forma que se asegure que la privacidad del usuario final se tiene en cuenta y se protege durante la vida del producto y el proceso de negocio de la aplicación.**	Cada entidad que recopila información personal sobre los usuarios, tiene que asegurarse de que se asigna a un representante (o representantes) de la empresa, la responsabilidad de garantizar que la privacidad del usuario final se preserva en las aplicaciones y servicios y procesos de negocio.	
RE2 **Dé a los usuarios las herramientas para que informen sobre los problemas que afecten a una aplicación.**	Los usuarios tienen que poder informar sobre los problemas con las aplicaciones o con sus contenidos o con las mismas plataformas de las aplicaciones. Los usuarios tienen que tener a su disposición información explicando cómo pueden reportar a aquellas aplicaciones de las que sospechan o saben fehacientemente que han violado la privacidad y seguridad de su información personal. Deben ser establecidos y mantenidos procedimientos para tratar esos informes e identificar cualquier amenaza o riesgos específicos.	Proporcione un breve informe y enlácelo con la página de inicio de la aplicación y/o con su página web corporativa. Indíquelo claramente. Si recopila direcciones de correo electrónico (con permiso) puede también enviar un email con esta información a los usuarios.

Si desea más información póngase en contacto con:

Natasha Jackson
Jefa de Políticas de Contenidos, GSMA
njackson@gsm.org

Pat Walshe
Director de Privacidad, GSMA
pwalshe@gsm.org

www.gsma.com/mobileprivacy